

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

FACEBOOK, INC.

Plaintiff,

v.

BRANDTOTAL LTD., et al.,

Defendants.

Case No. 3:20-CV-07182

DECLARATION OF MIKE CLARK

1 I, Mike Clark, declare:

2 1. I submit this declaration in support of Facebook's Opposition to Defendants' *Ex*
3 *Parte* Motion for Temporary Restraining Order in the above-captioned matter. I have personal
4 knowledge of the facts set forth herein, and if called to testify as a witness, I could do so
5 competently under oath.

6 2. I am a Director of Product Management at Facebook. In that role, I am personally
7 involved in Facebook and Instagram's (collectively "Facebook") efforts to prevent data scraping on
8 the Facebook and Instagram platforms. My team investigates potential violations of Facebook's
9 terms and policies, and works with Facebook's policy and legal teams to enforce those policies when
10 we determine they have been violated.

11 3. "Scraping" refers to the unauthorized automated extraction of user data. Scraping can
12 be either "logged-in" or "logged-out." Logged-in scraping involves scraping of data that is behind
13 password protection; logged-out scraping involves scraping of data available even without a
14 password. Logged-in scraping can be difficult to identify and distinguish from other activity by the
15 users.

16 4. Facebook restricts access to its website to authorized users who are logged-in for the
17 purpose of expressing themselves, engaging with one another, and forming communities. Facebook
18 restricts third-parties from using its service without authentication or logging-in, in order to protect
19 its service and users. Facebook has approved means for users to share data with third-parties, such
20 as through distinct Application Programming Interfaces ("APIs"). Facebook does permit third-
21 parties, such as authorized developers and businesses, to use certain APIs as an access point to get
22 data into and out of the Facebook platform with user consent. Third-party developers and businesses
23 with apps or managed services for Facebook must also abide by Facebook's Terms and Platform
24 Policies.

25 5. Scraping is a serious concern for technology companies and platforms, including
26 Facebook, for many reasons. For example:

27 a. Tools designed to scrape can often be used for other bad purposes. Most websites that
28 attempt to defend against scraping have limitations in place that would restrict access

1 or the ability to make unauthorized automated requests. Technologies designed to
2 circumvent these restrictions inherently make the sites less secure and can often be
3 used for other harmful acts, like coordinated inauthentic behavior or submitting
4 fraudulent content takedown requests. Scraping evades system limits and makes it
5 more difficult to employ technological solutions and systems that are designed to
6 detect and differentiate normal user behavior from automated activity, including that
7 caused by malware and other hacking tools.

- 8 b. The use of unauthorized automation to extract data from degrades public trust and
9 confidence. Users rightfully expect companies like Facebook to implement access
10 and scraping restrictions.
- 11 c. Scraping has adverse effects on privacy, free expression, and creative endeavors. A
12 user may provide data to a particular platform based on their trust that the platform
13 will maintain control of their data. Scraped data can include personal and private data
14 as well as content, like photographs, protected by copyright. And while users who
15 install scraping extension may in theory have consented to the collection of their
16 personal information, others who may use shared computers—family members,
17 roommates, friends—have not so consented and may not even be aware that their
18 personal information is being scraped. In the case of advertisements and ad creatives,
19 although advertisement on Facebook are considered publicly viewable, the creative
20 content belongs to the user that created and posted the advertisement, not the user that
21 views the advertisement.
- 22 d. Scraping takes away users’ control of their data. Facebook has a direct relationship
23 with a user and commits to protecting the users’ data from unauthorized users of its
24 website, such as scrapers. Facebook’s third-party APIs are the authorized method by
25 which Facebook can confirm that its users have consented to a third-party’s collection
26 of their data from Facebook.
- 27 e. Due to their inherent commercial nature, ads often involve licensed copyrighted
28 works. When the content of a user’s advertisement is improperly scraped and

1 removed from Facebook, the user who created the advertising content, including the
2 text and image used in the advertisement, has no ability to consent to its collection
3 and removal from Facebook. If the URL for the advertisement is scraped, both users
4 and non-users who have access to the advertisement URL can access and view the
5 advertisement and advertising metrics even if they were not part of the advertisements
6 intended audience. As a result, scraping can disaggregate content from the creator
7 leading to repeated misuse of proprietary material without credit or payment to the
8 creator.

9 f. Evasion of Facebook's anti-scraping terms or measures also undermines the integrity
10 and operation of its network. Unauthorized automated requests for data, in
11 circumvention of system limits, can burden the systems that support the service,
12 causing slow speeds, limiting functionality, and overall consuming computer
13 processing power intended to keep the network running. This also imposes costs on
14 Facebook because of the infrastructure needed to respond to the automated requests.
15 It also degrades the service being provided to real users.

16 g. Scraping can raise security concerns. Once data is scraped it can be used in ways that
17 users would never have expected when the user posted that content or provided that
18 data to a platform. It can put data in the hands of bad actors. For example, databases
19 of scraped personal information can provide bad actors an easy way to target
20 fraudulent communications. This can be true even if the user information is
21 deidentified or aggregated.

22 For at least these reasons, almost all platforms have terms or policies against scraping, and take
23 affirmative steps to enforce those policies, technologically and/or legally.

24 6. Facebook prohibits scraping of user data in their terms and employ a number of
25 technical measures to detect and disrupt scraping. Facebook makes a substantial investment in
26 technological solutions and policy efforts to prevent scrapers from improperly extracting user data
27 through automation. Facebook maintains a variety of systems that monitor and detect suspicious
28 activity on its website and restrict unauthorized automation from both logged-in and logged-out

1 scrapers. For example, Facebook limits the responses to server calls when we detect that behavior
2 may be automated. Facebook also detects and disrupts unauthorized automated requests on its
3 system by monitoring use patterns that are inconsistent with a human user, using challenge-response
4 tests to determine whether a computer user is human or not, and disabling accounts engaged in
5 automated activity.

6 7. Beyond these technical measures, Facebook has, and enforces, its policies against
7 scraping. The Facebook Terms of Service expressly prohibit users to “access or collect data from
8 our Products using automated means (without our prior permission) or attempt[s] to access data that
9 you do not have permission to access.” Likewise, Instagram’s Terms of Use explicitly prohibit all
10 Instagram users from “creating accounts or collecting information in an automated way without our
11 express permission.” Any user of either the Facebook or Instagram Platform must abide by the terms
12 of service that govern the particular platform. I understand that Michael Duffey has submitted a
13 declaration identifying and attaching the relevant Terms of Service.

14 8. Facebook’s anti-scraping policies are part of Facebook’s attempt to strike a careful
15 and thoughtful balance between protecting user data and offering platform access to authorized
16 third-parties. Facebook devotes substantial resources and works constantly to enforce its anti-
17 scraping policies against anyone who engages in unauthorized extraction of user data.

18 9. The Facebook policies against scraping are important to protect user data. Although
19 not every instance of scraping constitutes malicious behavior, I understand that it can be difficult to
20 determine whether scraping is engaged in for benign or malicious purposes. Facebook therefore
21 enforces its anti-scraping policies regardless of who is doing it or how they are using the scraped
22 information. Facebook does not authorize users or developers to deviate from the terms of service.

23 10. Even beyond the security considerations as they relate to its user, Facebook’s right to
24 enforce its policies against scraping is important to protect user privacy more broadly by maintaining
25 the integrity of its platform for the reasons I described above, and to deter third parties from
26 engaging in unauthorized conduct.

27 11. And in addition to all of the considerations described above, processing personal data
28 consistent with user expectations is essential to complying with modern data protection law and

1 regulation. It is therefore in the public interest for companies collecting personal data to properly
2 limit unauthorized extraction and collection of that data through methods that are inconsistent with
3 the purpose and scope of the original disclosure. To do so, companies must be able to guarantee to
4 their users that they will only grant access to data in ways consistent with the user's expectations.
5 Prohibiting companies such as Facebook from implementing technological and legal safeguards for
6 user data is not only against the individual users' interests, it could also subject Facebook to fines or
7 suits in many jurisdictions around the world.

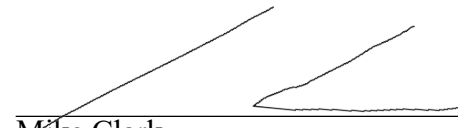
8 12. These concerns are not hypothetical. Facebook entered into a widely-publicized \$5
9 billion settlement with the Federal Trade Commission resulting in a consent decree ordering
10 Facebook to implement certain procedures to further enhance consumer protection and user privacy.
11 A copy of the Federal Trade Commission Order is attached hereto as Exhibit 1. In compliance with
12 the Federal Trade Commission Order, Facebook is required to report scraping covered incidents to
13 the FTC. Based on the investigation done in this case (I understand that Sanchit Karve has
14 submitted a declaration describing the investigation and findings), the browser extensions distributed
15 and used by BrandTotal and Unimania qualify as scraping covered incidents and will be reported to
16 the FTC. Failure to do so would subject Facebook to penalties.

17 13. As a result of the above-mentioned investigation, we observed that Defendants were
18 engaging at least two methods of scraping, which included (i) logged-in scraping by using the users'
19 browser as a proxy, and (ii) misappropriating session tokens and user's session IDs, through their
20 app, and then using them to gain access to Facebook to engage in logged-in scraping of user data.
21 BrandTotal and Unimania's access to the Facebook and Instagram platforms has been revoked for
22 violating Facebook's terms and policies against scraping. Facebook is not improperly enforcing
23 against BrandTotal and Unimania.

24 14. Our enforcement process can give developers an opportunity to work with Facebook
25 to address and remediate violations of our terms and policies. Those who provide fulsome
26 cooperation, and whose violations are of a nature that do not require their outright ban from the
27 platform, can sometimes have their access reinstated. I have personally been involved in multiple
28 enforcement actions in which a developer was able to bring themselves into compliance with

1 Facebook's terms and policies such that Facebook was able to restore access. In this case, I am
2 unaware of a request from BrandTotal and Unimania to access Facebook's platform for the purpose
3 of collecting data through . Instead, I only aware of BrandTotal' and Unimania's collection of data
4 through illegitimate means.

5
6 I declare under penalty of perjury that the foregoing is true and correct. Executed at Oakland,
7 California on the 21 day of October, 2020.

8
9 
Mike Clark